

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA)	
)	
Plaintiff,)	No. 5:18 CR 448
)	
v.)	AFFIDAVIT OF TAMI LOEHRS
)	
PHILIP M. POPA, JR.)	
)	
Defendant.)	

I, TAMI L. LOEHRS, hereby declare as follows:

1. I am a digital forensics expert and owner of Loehrs Forensics, LLC (formerly Loehrs & Associates) a firm specializing in digital forensics. My offices are located at 3037 West Ina, Suite 121, Tucson, Arizona 85741. I am competent to testify and the matters contained herein are based on my own personal knowledge.

2. I have been working with computer technology for over 20 years and I hold a Bachelor of Science in Information Systems. I have completed hundreds of hours of forensics training including courses with Guidance Software and Access Data. I am an EnCase Certified Examiner (EnCE), an Access Data Certified Examiner (ACE), a Certified Computer Forensic Examiner (CCFE) and a Certified Hacking Forensic Investigator (CHFI). I have conducted hundreds of forensics exams on thousands of pieces of evidence including hard drives, cell phones, removable storage media and other electronic devices. I have conducted seminars on Computer Forensics and Electronic Discovery throughout the United States. In addition, I hold a Private Investigator Agency License in the State of Arizona which requires a minimum of 6,000 hours investigative experience. My Curriculum Vitae is attached as Exhibit A.

3. I have been the digital forensics expert for the defense on over 500 child pornography cases throughout the United States and internationally since the year 2000 and have testified over one hundred and twenty times in State, Federal and international Courts.

4. I was contacted by Andrea Whitaker, counsel for Defendant Philip Popa, on February 1, 2019, to facilitate retaining my services for the purpose of assisting with matters related to the searching, collecting, analyzing and producing of electronic evidence in this matter.

5. I have reviewed discovery materials including, but not limited to, Affidavit of FBI Task Force Officer Ryan D. Anschutz dated July 19, 2018, FBI 302's documenting the investigation, execution of the search warrant, and arrest of Mr. Popa, Investigation Protocol Report, and the Indictment.

6. According to the Affidavit of Officer Anschutz, this case originated in April, 2018 when "a computer running Freenet software, with an IP address of 173.90.126.69, with 13.1 peers, requested from a law enforcement computer 136 out of 1786 total pieces needed to assemble a file with a SHA1 digital hash value of ATLOOVASIDQV6JPNOK4Z3MTKWGYFYS6W." That is, the computer at the suspect IP address reportedly requested less than .075% of a file which would likely render that file non-viewable and would not, in that **incomplete** state, contain child pornography. Officer Anschutz then downloaded the **completed** file from someone other than the suspect and describes the content of the **completed** file in his Affidavit. This activity occurred for several additional files, none of which the suspect reported having 100% of the content.

7. I have worked on hundreds of cases throughout the country involving law enforcement's investigations of P2P and BitTorrent file sharing networks, including the use of Freenet, which has brought to light serious issues with regard to the accuracy and reliability of the proprietary software used by law enforcement to conduct these investigations and whether that software is going beyond information that is publicly available as well as reporting false information regarding files that do not exist on a suspect computer and/or do not contain child pornography.

8. One of the primary issues with law enforcement's investigations of file sharing networks is their use of hash values to identify and describe files that they claim exist at a suspect's IP address.

9. A hash value is synonymous with a SHA1 value which is a mathematical algorithm that converts data into a small datum, usually a single integer. Essentially, a hash value is a file's signature and no two files should have the same signature. Any change in the file's data would result in a different hash value. As such, a partially downloaded file would not have the same hash value as the same file that had completed the download process. The file name itself does not affect the hash value. Therefore, two identical files may have different file names but the hash values will match. Conversely, two files with identical file names but different content will have different hash values.

10. While it is true that a hash value is essentially a file's fingerprint, this is only true if the file has actually been hashed. That is, anytime a single bit of data changes on a file, the algorithm must be recalculated and a new hash value is created. However, relying on hash values to identify a file becomes problematic when those files are downloaded with file sharing software on P2P networks because the files are not constantly hashed.

11. When a user downloads a file using a P2P file sharing application, whether on purpose or inadvertently, the file name and hash value is recorded inside of a system file associated with that P2P file sharing software installed on the computer. The hash value recorded is that of the completed file and does not provide an accurate signature of the actual content of the file because it takes time to download. For example, if I accidentally select a ten-minute video for download but then cancel the download immediately, my computer will have the file name and hash value of the completed ten-minute video. However, the actual video file on my computer is empty because no content was downloaded prior to cancelling the process. In that regard, it would be inaccurate to conclude that I had child pornography when I only had the hash value and file name but no viewable video.

12. In order for a file in the process of downloading to have a hash value that accurately represents its content, the file would have to be continually hashed during the download process. That is, every time a single bit of data changed during the download process, the file would have to be re-hashed, the algorithm would change and thus, the recorded hash value would be different. Because numerous files can be downloaded simultaneously, it is not practical for the software to continually rehash every file during the download process and would likely cause problems with the computer's performance if this were to occur. Therefore, the software simply records the hash value for each of the files in their anticipated completed state regardless of the state in which they actually exist on the computer (ie: empty, partial, corrupted, deleted, etc.)

14. Many files never complete the download process for reasons including, but not limited to, the user cancels the download because they don't want the file, the file was not complete on the source computer and therefore could not be downloaded, the file is corrupted, the connection was lost, etc. As such, the user ends up with file names and hash values on their computer that represent files in their completed state, even though the files themselves were never fully downloaded and/or never existed on the user's computer. That is, files that a user may have never intended to possess and that don't actually contain child pornography (including empty, incomplete, corrupted and even deleted files) will leave behind file names and SHA values of the completed versions of those files.

15. The use of file sharing software in and of itself comes with hidden dangers including mass downloading, files piggy-backing on other files, viruses, Trojans, hackers and other vulnerabilities that may cause a user to have file names, hash values and even files they did not want or did not intend to have. Even the most careful user who immediately recognizes and deletes unwanted content retains remnants of the unwanted activity such as file names and SHA values that may be falsely identified as illegal material during an undercover investigation. Unless files are actually downloaded from the suspect computer and viewed, it would be

impossible to say with any certainty which of those file names and SHA values represent remnants of unwanted material and which of those file names and SHA values represent actual files with illegal content. In spite of this, Officer Anschutz avers in his Affidavit that the IP address associated with Mr. Popa contains child pornography based on incomplete files reported by his law enforcement tool and then describes completed files that he downloaded from other sources.

16. In a subsequent report prepared by Officer Anschutz in July, 2018, he indicates that “law enforcement’s tool” analyzed the network and reported that it is significantly more probable than not that the suspect IP address (Mr. Popa) was the original requestor of the child pornography files. However, Officer Anschutz provides no information regarding “law enforcements tool”, including whether that tool has been tested and validated, nor does he provide any log files created by the law enforcement tool as foundation for his opinions. I know from experience on hundreds of cases that law enforcement’s proprietary tools create log files documenting activity which could be analyzed to corroborate or refute Officer Anschutz’s conclusions. I also know from experience on Freenet cases, that Freenet creates detailed logs of activity that could be analyzed to corroborate or refute Officer Anschutz’s conclusions although no Freenet logs have been produced to my knowledge.

17. It is critical to Mr. Popa’s defense to understand how law enforcement’s proprietary tool functions in order to determine its reliability and accuracy in identifying files that Officer Anschutz claims originated from Mr. Popa’s IP address.

18. In order to understand the importance of testing and validating software, one must have a basic understanding of software. In simplest terms, software is a set of instructions or commands telling a computer what to do (i.e.: source code). Those instructions or commands are written by people using high-level programming language and can encompass any task imaginable from basic computer operating functions to malicious activity meant to harm and disrupt. Programming is inherently complicated and humans are fallible. Therefore, when

analyzing how a piece of software functions, one must not only consider the “best-case scenario”, but the “what-if” scenario. In that regard, simply reviewing source code and identifying what it “should do” is not a substitute for actual testing and validation. In my experience, the best method with which to test and validate a piece of software is to apply the scientific method which is based on observation and experimentation. Similar to how scientists test a hypothesis, testing software involves running experiments with that software and analyzing the results.

19. Software testing and validation is the process of ensuring that the instructions or commands written by people fulfill their intended purpose without faults, failures or malfunctions. And software testing and validation is unequivocally necessary because people make mistakes. With mission-critical software that must perform flawlessly, such as software used in medical devices and nuclear facilities, testing and validation methods are meticulously documented by organizations such as the FDA and the U.S. Department of Energy. Less critical software applications such as publicly available open source software like BitTorrent do not have formal testing and validation requirements because any failure or malfunction is typically unimportant. However, basic principles of software testing and validation have been used in the software industry for over 20 years and applicable software testing tenets include:

- A good test case has a high probability of exposing an error;
- A successful test is one that finds an error;
- There is independence from coding;
- Both application (user) and software (programming) expertise are employed;
- Testers use different tools from coders;
- Examining only the usual case is insufficient;
- Each new version requires independent testing.

20. In my forensic training, some of which has come directly from law enforcement, I have been taught that I cannot rely on a tool (software) that has not been properly tested and validated by me and is not available for testing and validation by my industry peers. This is why most forensic examiners use tools like EnCase and FTK because they are industry standard tools

that are available for testing and validation by anyone and, as such, have been accepted by the Courts as viable tools. However, even those tools have been proven to produce inaccurate and unreliable data at times which has only been discovered through the ability to test and validate them.

21. The biggest challenge with developing an accurate tool is the diversity of data being collected and analyzed. This is why even tools like EnCase and FTK sometimes produce inaccurate and unreliable results. No two computer systems are identical. Computers are installed with different operating systems and there are hundreds of different versions of the same operating system, some are updated regularly and some are not updated at all. Those operating systems have thousands of different settings that can make each system unique in how it functions and records data. Within those operating systems a user can install millions of different software applications from large commercially produced software to small home-made software applications. Software applications may have bugs, data can be corrupted or incomplete, computers can be infected with viruses, Trojans and other malware. All of these variables have an effect on how that data is collected, analyzed and documented by a tool. While a tool may provide accurate information on an updated Windows system without any malware, the same tool may yield false results on a system that has not been updated and is infested with viruses.

22. Although Officer Anschutz makes sworn statements about the existence of child pornography at Mr. Popa's IP address without ever downloading the completed files, and draws conclusions about the files originating from that IP address without producing any data or foundation for those conclusions, I am unable to corroborate or refute Officer Anschutz's findings until I am able to independently examine all electronic data supporting those conclusions. I would anticipate needing approximately 40 hours to conduct a forensic examination of the evidence, prepare a detailed report and supplement this Affidavit if

necessary. In order to expedite such an examination and save the Court money, the evidence could be sent to the FBI facility in Phoenix where Loehrs Forensics maintains a local office.

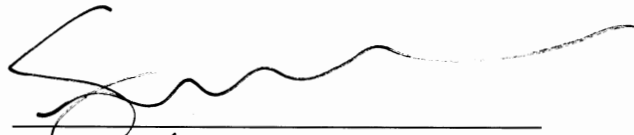
23. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

DATED: February 6, 2019.


TAMI LOEHRS

SUBSCRIBED AND SWORN to before me this 6 day of February, 2019




NOTARY PUBLIC

TAMILOEHRS

LOEHRS
f o r e n s i c s3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

EDUCATION	University of Arizona - Business Administration Pima College - Legal Assistant Sciences University of Phoenix - Bachelor of Science, Information Systems (With Honors)
CERTIFICATIONS AND LICENSES	Licensed Private Investigator, AZ Department of Public Safety, License No. 1594838 EnCase Certified Examiner (ENCE), Guidance Software (Since 2005) Access Data Certified Examiner (ACE) (Since 2008) Computer Hacking Forensic Investigator (CHFI) (Since 2010) Certified Computer Forensic Examiner (CCFE) (Since 2011)
SPECIALIZED TRAINING	EnCase Incident Response, Forensic Analysis and Discovery Course Arizona Semi Annual Conference Computer Crimes / Internet Fraud Access Data Boot Camp Access Data Windows Forensics How to Create and Perform Effective Keyword Searches Cell Phone Forensics Email Investigations File Recovery Through Data Carving Basic Investigations of Windows Vista Reverse Engineering Malware Incident Investigations Examining the Windows Registry Investigating Linux from a Forensic and Incident Response Perspective MySpace Investigations Cyber child Exploitation I - Investigations in the Workplace Mastering Conditions Forensics File Identification and Recovery Using Black-Hashed Hash Analysis Case Study Firefox Artifacts and Unallocated Space Hacking Malware Technical Profiling for Law Enforcement and Intelligence Vista Deep Dive I - Basic Investigations of Windows Vista Vista Deep Dive III - File and Registry Virtualization Malicious Artifacts Identification and Analysis Essential Macintosh Forensics FTK Transition 1.7 to 2.0 ACE Prep Computer Forensics and Ethical Hacking IOS Forensics – A comprehensive Approach Mac OS X Lion Forensics Update Tracks Left by Covering Your Tracks What's New in Windows Forensics A Forensic Look at Windows 8 Immersive Applications: What's Behind the Tiles Smart Device App Analysis Windows 8 File History Artifacts Ares and LimeWire Pro Peer to Peer Files Sharing Software Analysis Mac OS X Delving a Little Deeper Vehicle Systems Forensics How to Catch an Insider Data Thief Forensic Testimony in Court Ubiquity Forensics – Your iCloud and You Searching in EnCase 8 with EQL Digital Evidence from Social Networking Sites & Smartphone Apps

TAMI LOEHRS

LOEHRS
f o r e n s i c s3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Digital Forensic Child Exploitation Investigations
 Smartphones: The Nexus of Evidentiary Data from Social Media to IoT
 How Artificial Intelligence is Becoming a Crucial Tool for Next Generation Law Enforcement
 Accelerate in Action: Email Investigation Methods with Hillary Clinton's FOIA Release
 Jurisdiction in Cyberspace: A Question of Conflict of Laws?
 Damaged Device Forensics Complimentary
 Memory Forensics - Hunting Malware

PROFESSIONAL
EXPERIENCE**Computer Forensics Examiner**

Loehrs Forensics, LLC. (Formerly Loehrs & Associates, Inc.)

Computer forensics services, particularly pertaining to legal evidence, including forensic acquisitions of digital artifacts including computers, cell phones, removable storage media, digital cameras, gaming consoles, etc.; data collection and recovery from allocated and unallocated space; data analysis and conclusions regarding who, what, when, where and how data came to be on an artifact; detailed reporting of conclusions and analysis; and testimony regarding forensic procedures, analysis and conclusions.

Technical experience also includes all aspects of information technology including designing, implementing, maintaining and troubleshooting networks; building and repairing computer systems including workstations and servers; software implementation and support for hundreds of applications; programming; configuring, maintaining and troubleshooting switches and routers; Internet services and web design; designing, maintaining and troubleshooting backup and disaster recovery systems.

PROFESSIONAL
MEMBERSHIPS*Forensic Expert Witness Association (FEWA)*

Member of the Arizona Chapter

Based in San Francisco, the Forensic Expert Witness Association (FEWA) is the only non-profit professional membership organization that verifies that each of its professional members has testified at least three times as an expert witness. FEWA is dedicated to the professional development, ethics and promotion of forensic consultants in all fields of discipline. FEWA provides professional education for experts of all levels of experience and also for those aspiring to be experts who have not yet testified, which spans all technical specialties.

National Association of Public Defense (NAPD)

Organizational Membership

The National Association for Public Defense (NAPD) engages all public defense professionals into a clear and focused voice to address the systemic failure to provide the constitutional right to counsel, and to collaborate with diverse partners for solutions that bring meaningful access to justice for poor people. NAPD currently unites nearly 7,000 practitioner-members across the country into a cohesive, unwavering, irrepressible community capable of bringing justice to a broken system.

TESTIFYING
EXPERIENCE**Trials: 52****Hearings: 72**

Trial: USDC, District of Arizona
 Child Pornography
 Attorney: Barbara Hull
 Case No. CR1701311-PHX-DGC

Trial: USDC, District of Arizona
 Child Pornography
 Attorney: Philip Seplow
 Case No. CR1701107-01-PHX-SPL

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Hearing: USDC, District of Arizona
Child Pornography
Attorney: Philip Seplow
Case No. CR1701107-01-PHX-SPL

Trial: USDC, District of Arizona
Child Pornography
Attorney: David Eisenberg
Case No. CR 16-08202-PCT-ROS

Hearing: USDC, District of Arizona
Child Pornography
Attorney: Stephanie Bond
Case No. 4:16-CR-00046-RCC-DTF

Hearing: USDC, Central District of California
Probation Violation
Attorney: Callie Steele
Case No. CR08-00106-CBM

Hearing: Escambia County Circuit Court, Florida
Child Pornography
Attorney: John Beroset
Case No. 2016 CF 5144

Hearing: Mohave County Superior Court, Arizona
Child Pornography
Attorney: Virginia Crews
Case No. CR-2015-00312

Hearing: Maricopa County Superior Court
Child Pornography
Attorney: Phillip Beatty
Case No. CR2015-131645-001DT

Hearing: USDC, District of Arizona
Bank Fraud, Aggravated Identity Theft, Transactional Money Laundering
Attorney: Ashley Adams
Case No. CR-14-01066-PHX-DJH

Hearing: Escambia County Circuit Court, Florida
Child Pornography
Attorney: John Beroset
Case No. 2016 CF 5144

Hearing: Bradford County Court of Common Pleas, Pennsylvania
Child Pornography
Attorney: Kristina Supler
Case No. CP-08-CR-000141-2016

Hearing: Orleans Criminal District Court, Louisiana
Child Pornography

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Attorney: Herbert Larson
Case No. 523-930

Hearing: Mohave County Superior Court, Arizona
Child Pornography
Attorney: Virginia Crews
Case No. CR-2015-00312

Hearing: Maricopa County Superior Court, Arizona
Child Pornography
Attorney: Cindy Castillo
Case No. CR 2014-002842-001

Hearing: Chester County Justice Center, Pennsylvania
Child Pornography
Attorney: Adam Bompadre
Case No. Juvenile Court

Hearing: USDC, Central District of California
Child Pornography
Attorney: James Riddet
Case No. SACR14-00188

Hearing: USDC, District of New Hampshire
Child Pornography
Attorney: Bjorn Lange
Case No. CR15-110-01-PB

Hearing: Court of Common Pleas, Lackawanna County Pennsylvania
Child Pornography
Attorney: Robert Trichilo
Case No. 20161048

Trial: Court of Common Pleas, Lackawanna County, Pennsylvania
Child Pornography
Attorney: William Peters
Case No. CR-2013-2694-35

Hearing: USDC, Central District of California
Child Pornography
Attorney: Craig Harbaugh
Case No. CR 15-224-DMG

Hearing: Second Judicial District Court Weber County, Utah
Child Pornography
Attorney: Tara Isaacson
Case No. 131901792

Hearing: USDC, Central District of California
Probation Violation
Attorney: Kim Savo
Case No. CR 06-911-ODW

TAMI LOEHRS

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

LOEHRS
f o r e n s i c s

Hearing: USDC, Western District of Missouri
Child Pornography
Attorney: Kristin Jones
Case No. 13-03081-01-CR-S-MDH

Hearing: Second Judicial District Court Weber County, Utah
Child Pornography
Attorney: Tara Isaacson
Case No. 131901792

Trial: USDC, Southern District of California
Child Pornography
Attorney: Michael Crowley
Case No. CR-03447

Trial: Lancaster County Court of Common Pleas, Pennsylvania
Child Pornography
Attorney: Adam Bompadre
Case No. CR-0000336-2015

Hearing: Lancaster County Court of Common Pleas, Pennsylvania
Child Pornography
Attorney: Adam Bompadre
Case No. CR-0000336-2015

Hearing: USDC, Central District of California
Child Pornography
Attorney: Cuauhtemoc Ortega
Case No. CR 15 00063

Hearing: Maricopa County Superior Court, Arizona
Child Pornography
Attorney: Craig Gillespie
Case No. CR2014-005922-001

Trial: Yavapai County Superior Court, Arizona
Luring of a Minor
Attorney: Michael Alarid
Case No. CR201300970

Hearing: Pima County Superior Court, Arizona
Divorce
Attorney: Nicole Hinderaker
Case No. N/A

Trial: Pima County Superior Court, Arizona
Child Pornography
Attorney: Paul Skitzki
Case No. CR-20141915

Trial: Pima County Superior Court, Arizona

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Child Pornography
Attorney: Tatiana Struthers
Case No. CR20111156-001

Hearing: The University of the State of New York Education Department
Determination of Good Moral Character
Attorney: Carolyn Gorczynski
Case No. N/A

Hearing: USDC, Central District of California
Child Pornography
Attorney: James D. Riddet
Case No. SACR14-00188

Hearing: USDC, Eastern District of California
Child Pornography
Attorney: Michael Chastaine
Case No. 2:12-CR-0401 KJM

Hearing: Yavapai County Superior Court, Arizona
Child Pornography
Attorney: Michael Alarid
Case No. CR201300970

Trial: Essex Superior Court, Massachusetts
Child Pornography
Attorney: Mark Schmidt
Case No. ESCR09-1514

Trial: San Francisco Superior Court, California
Impersonating Police Officer and Coercing Sex Acts
Attorney: Phoenix Streets
Case No. 14025591

Trial: In the Crown Court at Kingston
Child Pornography
Attorney: Alex Chowdhury
Case No. 01TW0018610/1

Hearing: USDC, District of Nebraska
Child Pornography
Attorney: John H. Rion
Case No. 8:13CR107

Trial: County of Bernalillo District Court, New Mexico
Homicide
Attorney: Thomas M. Clark
Case No. D-202-CR-2012-03537

Trial: New Castle County Superior Court, Delaware
Child Pornography
Attorney: Thomas Foley

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Case No. 13-01-011058

Trial: Snohomish County District Court, Washington
Child Pornography
Attorney: Sarah Silbovitz
Case No. CR13-1-01219-1

Hearing: New Castle County Superior Court, Delaware
Child Pornography
Attorney: Thomas Foley
Case No. 1310019248

Trial: Pima County Superior Court, Arizona
Homicide
Attorney: Paul Eckerstrom and Alicia Cata
Case No. CR20084012

Trial: USDC, Southern District of New York
Conspiracy, Wire Fraud
Attorney: Marlon Kirton
Case No.1:09-CR-01002-WHP

Hearing: USDC, District of New Mexico
Child Pornography
Attorney: Jon Paul Rion
Case No. 11CR-1690-MV

Trial: USDC, Eastern District of Pennsylvania
Child Pornography
Attorney: Mark Greenberg
Case No. CR12-228

Trial: Ontario Court of Justice, Central West Region, Canada
Child Pornography
Attorney: Antal Bakaity
Case No. SA 07 CR-267

Hearing: USDC, District of Vermont
Child Pornography
Attorney: David McColgin
Case No. 5:12-CR-44

Trial: Pima County Superior Court, Arizona
Child Pornography
Attorney: Katherine Estavillo
Case No. CR20102131-001

Trial: USDC, Western District of New York
Child Pornography
Attorney: Igor Niman
Case No. M-09-1129

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Hearing: Cochise County Superior Court, Arizona
Child Pornography
Attorney: Steve Sherick
Case No. CR2010-00305

Hearing: Maricopa County Superior Court, Arizona
Homicide
Attorney: Alan Tavassoli
Case No. 2009-030306-001 SE

Hearing: Pima County Superior Court, Arizona
Child Pornography
Attorney: Katherine Estavillo
Case No. CR-20102131-001

Trial: USDC, Northern Mariana Islands
Child Pornography
Attorney: Samuel Mok
Case No. 12-00017

Trial: USDC, Western District of Texas
Child Pornography
Attorney: Luis Islas
Case No. 12-CR-217

Hearing: USDC, Western District of Texas
Child Pornography
Attorney: Luis Islas
Case No. 12-CR-217

Trial: Yuma County Superior Court, Arizona
Homicide
Attorney: Kristi Riggins
Case No. 1400CR2008-005

Hearing: Collin County Superior Court, Texas
Homicide
Attorney: Jim Burnham
Case No. 296-81605-2011

Hearing: USDC, New Mexico, Santa Fe Divisional Office
Child Pornography
Attorney: John Paul Rion
Case No. 11-23-6-0010

Hearing: USDC, Central District of California
Child Pornography
Attorney: Gary Dubcoff
Case No. CR 06-19 DSF

Hearing: USDC, Northern District of Georgia
Child Pornography

TAMILOEHRS

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

LOEHRS
f o r e n s i c s

Attorney: Ann Fitz
Case No. 1:11-CR-00067-RWS-JFK

Trial: Cochise County Superior Court
Child Pornography
Attorney: Tanja Kelly
Case No. CR201100293

Trial: USDC, District of Arizona
Hate Crime
Attorney: Barbara Hull
Case No. CR-09-712-PHX-DGC

Trial: USDC, Western District of Wisconsin
Fraud
Attorney: David Mandell
Case No. CR2011 0082

Trial: Superior Court of Forsyth County
Child Pornography
Attorney: Romin Alavi
Case No. 10CR-0118

Hearing: Cochise County Superior Court
Child Pornography
Attorney: Mark Beradoni
Case No. CR201000769

Hearing: USDC, Middle District of Louisiana
Child Pornography
Attorney: Michael Reese Davis, Sr.
Case No. 3-11-CR-000038-JJB-DLD

Trial: Pima County Superior Court
Child Pornography
Attorney: Paul Skitzki
Case No. CR-2010-2663

Hearing: Maricopa County Superior Court
Child Pornography
Attorney: Craig Gillespie
Case No. CR2009-114677001

Trial: USDC, Northern District of California
Computer Fraud
Attorney: Manuel Araujo
Case No. CR05-0812 RMW

Hearing: Pima County Superior Court
Child Pornography
Attorney: Katherine Estavillo
Case No. CR2010-1967

TAMILOEHRS

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

LOEHRS
f o r e n s i c s

Hearing: Forsyth County Superior Court
Child Pornography
Attorney: Romin Alavi
Case No. 10CR-0118

Trial: USDC, District of Maine
Child Pornography
Attorney: Theodore Fletcher
Case No. SA 07 CR-256

Trial: USDC, Northern District of California
Forgery
Attorney: Elizabeth Falk
Case No. CR10-0068

Hearing: Commonwealth Court of Pennsylvania
Child Pornography
Attorney: John Abom
Case No. CP-21-CR-724-20

Trial: USDC, District of Arizona
Child Pornography
Attorney: David Cantor
Case No. CR09-0794TUCJMR

Trial: USDC, Middle District of Alabama
Child Pornography
Attorney: Susan James
Case No. 2:09CR 73-MEF

Trial: USDC, District of Alabama
Child Pornography
Attorney: Tim Halstrom
Case No. 3:09-CR-159-WKW

Trial: USDC, District of Delaware
Child Pornography
Attorney: Luis Ortiz
Case No. 09-43-SLR

Settlement Conference: Maricopa County Superior Court
Child Pornography
Attorney: Adrian Little
Case No. CR09-000282

Sentencing Hearing: USDC, Northern District of Texas
Child Pornography
Attorney: Jim Burnham
Case No. 3:09-CR-339-M

Hearing: Maricopa County Superior Court

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Child Pornography
Attorney: William Foreman
Case No. CR2009-007925-001 DT

Civil Service Hearing: State of Arizona
Unauthorized Use of Computer
Attorney: Jeff Jacobson
Case No. C2009-8685

Hearing: USDC, District of Arizona
Child Pornography
Attorney: Leslie Bowman / Clint Liechty
Case No. CR-09-441-TUC

Trial: USDC, District of Arizona
Child Pornography
Attorney: Gary Kneip
Case No. CR-08-433

Hearing: USDC, District of Arizona
Child Pornography
Attorney: Harold Higgins
Case No. CR09-1322TUC

Trial: USDC, District of Arizona
Child Pornography
Attorney: Beau Brindley
Case No. 05-CR-931

Sentencing Hearing: USDC, District of Arizona
Child Pornography
Attorney: Neal Taylor
Case No. CR08-310-PHX-PR

Trial: USDC, District of California
Child Pornography
Attorney: Caro Marks
Case No. CR S-07-290 WBS

Trial: Commonwealth of Pennsylvania
Child Pornography
Attorney: Stanton Levenson
Case No. CR 458-07

Trial: USDC, District of New Mexico
Homicide
Attorney: Barbara Mandel
Case No. 07614-RB

Trial: Humboldt County Superior Court
Child Pornography
Attorney: Cathy Dreyfuss

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Case No. 55-08-001612

Trial: USDC, District of Georgia
Child Pornography
Attorney: Ann Fitz,
Case No. 2:08 CR000033

Hearing: Pinal County Superior Court
Harassment
Attorney: Morgan Alexander
Case No. CR2008-00286

Trial: Pima County Superior Court
Child Pornography
Attorney: David Euchner
Case No. CR2004-2573

Trial: USDC, District of California
Violating Terms of MySpace
Attorney: Dean Steward
Case No. CR-08-582-GW-001

Trial: USDC, District of Wyoming
Child Pornography
Attorney: Tom Smith
Case No. 07-CR-32-B

Trial: USDC, District of Puerto Rico
Child Pornography
Attorney: Victor Gonzalez-Bothwell
Case No. 07-140(CCC)

Trial: USDC, District of Arizona
Prostituting a Minor
Attorney: Barbara Hull
Case No. CR07-00871-001-PHX-ROS

Trial: USDC, District of Arizona
Child Pornography
Attorney: Ralph Ellinwood
Case No. CR05-1049-TUC-FRZ

Hearing: USDC, District of California
Child Pornography
Attorney: Rachelle Barbour
Case No. CR-S-07-0020

Hearing: USDC, 379th Judicial District, Bexar County Texas
Child Pornography
Attorney: Evelyn Martinez
Case No. 2006-CR-0477W

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Trial: USDC, District of Arizona
Child Pornography
Attorney: Laura Udall
Case No. CR06-0825

Trial: Coconino County Superior Court
Child Pornography
Attorney: Brad Bransky
Case No. CR2006-1045

Hearing: Pima County Superior Court
Murder
Attorney: Creighton Cornell
Case No. CR2007-0403

Hearing: Pima County Superior Court
Evidence Tampering
Attorney: Todd Jackson
Case No. C2006-5273

Hearing: Maricopa County Superior Court
Child Pornography
Attorney: Jason Lamm
Case No. CR2007-006060

Hearing: Coconino County Superior Court
Child Pornography
Attorney: David Bednar
Case No. CR2007-0519

Hearing: Maricopa County Superior Court
Child Pornography
Attorney: Gary Hendrickson
Case No. CR2006-171689-001

Trial: USDC, District of Arizona
Can Spam
Attorney: Michael Black
Case No. CR05- 870PHX

Hearing: Maricopa County Superior Court
Child Pornography
Attorney: Mark Hawkins
Case No. CR2006-136640-001

Hearing: Navajo County Superior Court
Child Pornography
Attorney: David Martin
Case No. CV2005-013148

Hearing: Pima County Superior Court
IP Theft

TAMIL LOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Attorney: Todd Jackson
Case No. C2005-5273

Hearing: USDC, District of Arizona
Child Pornography
Attorney: Ralph Ellinwood
Case No. CR05-1049-TUC-FRZ

Hearing: USDC, District of Arizona
Child Pornography
Attorney: Steven West; Nesci, St. Louis & West
Case No. CR04-2351-TUC-JMR

Hearing: Maricopa County Superior Court
Child Pornography
Attorney: William Foreman
Case No. CR2004-007249-001 DT

Hearing: USDC, District of Arizona
Child Pornography
Attorney: Patricia Gitre
Case No. CR03-490-PHX-ROS

Hearing: Pima County Superior Court
Child Pornography
Attorney: Larry Rosenthal
Case No. CR2001-1155

Hearing: Pima County Superior Court
Child Pornography
Attorney: David DeCosta
Case No. CR2002-0171

Trial: Yuma County Superior Court
Child Pornography
Attorney: Richard Bock; Lingeman & Bock
Case No. S1400 CR2000-00472
CA CR02-0578

PRESENTATIONS

August, 2018: Speaker
Las Vegas Federal Public Defender
Digital Forensics
Las Vegas, Nevada

September, 2016: Speaker
Montana Criminal Defense Lawyers Association
Computer Forensics
Billings, Montana

July, 2016: Speaker
National Association for Public Defense

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Are Law Enforcement's Online Investigations Violating the 4th Amendment?
Tucson, Arizona

July, 2016: Speaker
National Association for Public Defense
How to Know When Digital Evidence has been Manipulated or Fabricated
Tucson, Arizona

May, 2016: Speaker
Association of Certified Fraud Examiners
Computer Forensics & Fraud
Albuquerque, New Mexico

September, 2015: Speaker
Arizona Information Defenders
Computer Forensics
Tucson, Arizona

September, 2015: Speaker
Association of Certified Fraud Examiners
Computer Forensics & Fraud
Tucson, Arizona

February, 2015: Speaker
Arizona Information Defenders
Computer Forensics
Tucson, Arizona

March, 2014: Speaker
Office of the Public Defender
Computer Forensics
San Francisco, California

August, 2013: Speaker
Office of the Public Defender
Computer Forensics for Sex Cases
Palm Beach Gardens, Florida

September, 2012: Speaker
Office of the Public Defender
Computer Forensics for Sex Cases
Fort Myers, Florida

June, 2012: Speaker
Annual APDA Statewide Conference
Computer Forensics for Sex Cases
Phoenix, Arizona

June, 2012: Speaker
Federal Community Defender for Eastern District of Pennsylvania
New Issues in Computer Forensics
Philadelphia, Pennsylvania

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

September, 2011: Speaker
Pima County Public Defender
Computer Forensics
Tucson, Arizona

April, 2011: Speaker
Delaware Federal Public Defender
Computer Forensics
Wilmington, Delaware

September, 2010: Speaker
Arizona Attorneys for Criminal Justice
Fall Seminar 2010
Digital Evidence
Tucson, Arizona

April, 2010: Speaker
Office of Defender Services
Conference for Federal Defender Computer Systems Administrators
Computer Forensics / LimeWire
Chicago, Illinois

January, 2010: Speaker
Administrative Office of the United States Courts
Sixth National Seminar on Forensics Evidence and the Criminal Law
Computer Forensics
San Diego, California

September, 2009: Speaker
Arizona Attorneys for Criminal Justice
Fall Seminar 2009
Computer Forensics, A Case Study
Tucson, Arizona

April, 2009: Speaker
Administrative Office of the United States Courts
Portland Winning Strategies Seminar
Computer Forensics
Portland, Oregon

April, 2008: Speaker
National Defender Investigator Association
National Conference
Computer Forensics
Las Vegas, Nevada

November, 2007: Speaker
Association of Legal Administrators
Region 6 Educational Conference & Exposition
E-Discovery and Potential Land Mines
Tucson, Arizona

TAMI LOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

October, 2007: Featured Speaker
Lorman Education Services
Computer Forensics and Electronic Discovery in Arizona
Tucson, Arizona

September, 2007: Featured Speaker
National Defender Investigator Association
Computer Forensics
Phoenix, Arizona

July, 2007: Featured Speaker
Federal Community Defender Office of Pennsylvania
Computer Forensics
Philadelphia, Pennsylvania

April, 2005: Speaker
Fennemore Craig
Electronic Discovery - A Case Study
Tucson, Arizona

March, 2005: Speaker
Arizona Court Reporters Association Annual Convention
Computer Forensics and Electronic Discovery
Phoenix, Arizona

March, 2005: Speaker
Morris K. Udall Inn of Court
Electronic Discovery
Tucson, Arizona

October, 2004: Featured Speaker
Tucson Association of Legal Assistants
Computer Forensics and Electronic Discovery
Tucson, Arizona

June, 2004: Vendor
Arizona State Bar Convention
Phoenix, Arizona

October, 2003: Featured Speaker
Arizona Association of Licensed Private Investigators (AALPI)
Computer Forensics and Electronic Discovery
Phoenix, Arizona

February, 2003: Featured Speaker
Arizona Association of Licensed Private Investigators (AALPI)
Computer Forensics and Computerized Litigation
Tucson, Arizona

October, 2002: Featured Speaker
Arizona Mystery Writers

TAMILOEHRS

LOEHRS
f o r e n s i c s

3037 West Ina, Suite 121 | Tucson, Arizona 85741
Ofc: 520.219.6807 | Email: TL@LoehrsForensics.com

Computer Forensics
Tucson, Arizona

January, 2002: Featured Speaker
Tucson Association of Legal Assistants
Computer Forensics and Computerized Litigation

July, 2001: Vendor
CLE by the Sea - Electronic Courtrooms, Discovery of Electronically Stored Information
San Diego, California

June, 2001: Featured Speaker
Technology for the Practice of Law
Tucson, Arizona

April, 2001: Vendor
State Bar of Arizona - Technology Show
Phoenix, Arizona

January, 2001: Featured Speaker
Internet Security Issues - Detection and Prevention
Tucson, Arizona